deltacom™ 7037 Old Madison Pike Huntsville, AL 35806

February 25, 2010

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Customer Proprietary Network Information Certification, WC Docket No. 06-36

Dear Ms. Dortch:

ITC^DeltaCom, Inc., on behalf of its operating subsidiaries, DeltaCom, Inc., and Business Telecom, Inc. and Interstate FiberNet, Inc. respectfully submit its Annual CPNI Certification and corresponding statement in the above-referenced docket.

Should you have any questions regarding this filing, please contact me at 256-382-7090.

Sincerely,

Traci Tidmore

Traci Tidmore
Regulatory Manager

Attachment

cc: Best Copy and Printing, Inc. (via email)

deltacom™ 7037 Old Madison Pike ▸ Huntsville, AL 35806 ▸

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2009

Date filed: February 22, 2010

Companies covered by this certification: DeltaCom, Inc., Business Telecom, Inc. and Interstate FiberNet, Inc.

Form 499 Filer ID: 807069, 808512 and 803136, respectively

Name of signatory: Michael Harry

Title of signatory: Senior Vice President, Customer Operations

I, Michael Harry, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has operating procedures and policies in place that are designed to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures are designed to maintain compliance with the CPNI rules. Please see attached accompanying statement.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Michael Harry

Date 2/22/2010

## Customer Proprietary Network Information Policy Statement - 2009

ITC^DeltaCom Inc., through its operating subsidiaries, DeltaCom Communications, Inc., Business Telecom, Inc. and Interstate FiberNet, Inc. (collectively, the "companies"), provides this statement pursuant to section 64.2009(e) of the Federal Communications Commission's rules, 47 C.F.R. § 64.2009(e), to summarize the operational procedures and policies in place that are designed to ensure compliance with the Commission's Customer Proprietary Network Information ("CPNI") rules.

**Use, Disclosure, or Access to CPNI**

Consistent with section 222 of the Communications Act of 1934, as amended (the "Act"), and the Commission's implementing rules, absent customer consent, the companies may use, disclose, or permit access to CPNI as follows:

(1) to protect our rights and property, our customers, and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, our services;

(2) to provide or market service offerings among the categories of service to which the customer already subscribes;

(3) for the provision of customer premises equipment;

(4) for billing and rendering services to the customer; and

(5) as required by law, such as in response to a validly issued subpoena.

**Use of CPNI for Marketing Purposes**

At present, we make limited use of CPNI to market our services. When CPNI is used, we maintain records of our sales and marketing campaigns for a minimum of one year. The records contain a description of each campaign, the CPNI that was used in the campaign, and the products and services that were offered as part of the campaign. We have established a supervisory review process governing the use of CPNI for outbound marketing. Under such a process, all sales personnel would be required to obtain supervisory approval before using CPNI for marketing purposes.

We may use, disclose or permit access to CPNI to market service offerings among the categories of service to which the customer already subscribes. When we provide different categories of service, and a customer subscribes to more than one service category, we may share the customer's CPNI with the affiliate that provides service to the customer. We do not share CPNI with third-parties for marketing purposes.

In the event that we seek to market services to customers outside of the category of services to which the customer subscribes, or for any purpose other than as permitted without customer approval or as required by law, we would solicit customer approval for such use of CPNI in accordance with the Commission's CPNI rules.

**Employee Training/Disciplinary Process**

Employees are trained to respect the privacy of customer information. We will take all necessary disciplinary actions for violation of this policy. For those employees with access to call-detail CPNI, particular emphasis has been placed on training related to the CPNI requirements that became effective on December 8, 2007.

**Authentication and the Release of Call Detail Information**

Procedures are in place to authenticate customers prior to disclosing CPNI based on customer-initiated telephone contacts and online. It is our policy to prohibit the release of call detail information during an in-bound call. Instead, we either call the customer back at the telephone number of record or send the requested call detail information to an established address of record. During the reporting period, we have been developing and implementing a system whereby access to online accounts is initially obtained through the use of a company-assigned personal identification number (PIN). The customer would then use the PIN to establish its own password, security hints, and back-up authentication. This is replacing the existing system in which customers are able to set-up an online account through the use of a valid account number and then establish their own password. As an additional security measure for online accounts, we periodically send via U.S. Postal Service to each retail customer's address of record a list of those e-mail addresses that have established access the customer's online account. This provides the customer the ability to verify that no unauthorized access to their online account information has occurred.

**Additional Security Protections**

We have implemented measures to protect against pretexting. Employees are instructed to notify designated personnel if they learn of activity that is indicative of pretexting. We also have implemented network security protections, including, but not limited to, encrypting certain data and data transmissions and limiting employee access to CPNI based on their need to access such data.

**Security Breaches**

We have implemented procedures pursuant to which we will notify the United States Secret Service and the Federal Bureau of Investigation (collectively, "law enforcement") within seven days of a reasonable determination of a breach of a customer's CPNI. Unless law enforcement directs otherwise, we will notify affected customers of the breach as soon as practicable after the expiration of the seven-business day waiting period. We will maintain a record in accordance with section 64.2011(d) of any breaches discovered, notifications made to law enforcement, and notifications made to customers for at least two years.

We will maintain a record of any actions taken against pretexters and will provide that information to the Commission in our annual certification. In the certification, we also will provide any information that our employees learn regarding the processes pretexters are using to attempt to obtain CPNI.

**Customer Complaints**

We have implemented a process to track customer complaints regarding the unauthorized use, disclosure, or access to CPNI. We log all customer complaints, including those pertaining to CPNI. If we receive complaints regarding CPNI, we will break them down by category, and provide a summary of the complaints in the annual certification that we provide to the Commission.